Incentive Regulation and Utility Benchmarking for Electricity Network Security

Rabindra Nepal*
School of Business, Charles Darwin University

Tooraj Jamasb**
Durham University Business School

Abstract

The incentive regulation of costs related to physical and cyber security in electricity networks is an important but relatively unexplored and ambiguous issue. These costs can be part of cost efficiency benchmarking or, alternatively, dealt with separately. This paper discusses the issues and proposes options for incorporating network security costs within incentive regulation in a benchmarking framework. The relevant concerns and limitations associated with the accounting and classification of network security costs, choice of cost drivers, data adequacy and quality and the relevant benchmarking methodologies are discussed. The analysis suggests that the present regulatory treatment of network security costs using benchmarking is limited to being an informative regulatory tool rather than being deterministic. We discuss how alternative approaches outside the benchmarking framework, such as the use of stochastic cost-benefit analysis and cost-effectiveness analysis of network security investments can complement the results obtained from benchmarking.

Keywords: benchmarking; network security; incentive regulation; exceptional events

JEL Classification: L94, L51, L98

**Corresponding author*. School of Business, Charles Darwin University, Email: rabindra.nepal@cdu.edu.au, Phone: +61 (0) 8 89468856.

** Durham University Business School, Mill Hill Lane, Durham, DH1 3LB, United Kingdom, Email: tooraj.jamasb@durham.ac.uk, Phone: +44 (0) 191 3345463.

Acknowledgement: *The authors acknowledge the financial support of the FP7-security project cofounded by the European Commission. The views expressed herein are those of the authors and can, therefore, in no way be taken to reflect the official position of the European commission. We are also grateful to the editor and the referee for guiding the improvements in this paper. The usual disclaimer applies.*

1. Introduction

The introduction of incentive-based regulation since market liberalization has coincided with a gradual adoption of cost and efficiency benchmarking as a regulatory instrument by many European energy regulators. For example, Norway introduced incentive regulation and efficiency benchmarking in 1997 while Germany followed suit in 2009. Benchmarking can be broadly defined as a comparison of some measure of actual efficiency and productivity performance against a reference or benchmark performance (Jamasb and Pollitt, 2000). The primary role of benchmarking under incentive regulation is to decouple the allowed revenues of a network utility from its own underlying costs by determining the regulated revenue cap based on the cost of efficient networks.

Benchmarking allows *comparative regulation* and uses *outside information* beyond what is revealed by the regulated network itself. Hence, benchmarking serves as a regulatory tool to eliminate or reduce the firm's asymmetric information (moral hazard and adverse selection) advantage with its operational and capital costs (*inputs*) and demand[1]. The use of available outside information in network regulation that is retrieved independently of the network companies implies that benchmarking, in effect, aims to mimic the incentive mechanisms of a competitive market in a monopoly environment. This resembles a yardstick competition in its extreme form where the outcomes of perfect competition are replicated in a regulated natural monopoly context (Shleifer, 1985).

However, the European electricity supply industry (ESI) is undergoing fundamental technical changes in the drive towards sustainability and ensuring the security of supply signalling changes in energy policy priorities from the overriding economic efficiency goals. Competitiveness, energy security and decarbonisation have become the main energy policy priorities post liberalisation (Pollitt and Haney, 2013). These changes have also sparked debate on how incentive regulation and the application of benchmarking within incentive regulation should evolve (Cambini et al., 2014). For example, it is estimated that the required costs of the transmission grid expansions in Europe will be in the region of 104 billion euros (ENTSOE, 2012). Similarly, the investment needs in Europe's distribution grid is estimated to be around 520 billion euros by 2035 in the transition towards a low-carbon economy (EURELECTRIC, 2012). These investments are driven by the need to accommodate rapid

[1] This is a typical information asymmetry problem arising in a principal-agent relationship where the regulated agent holds superior information on its own cost and demand structures than the principal (or the regulator in our case). See Laffont and Tirole (1993) for more details.

technological advances in distributed energy resources such as solar, energy storage, electric vehicles, micro-grids, intelligent home energy management, demand aggregation, and demand response, all leading to a complex future with a differing role for electricity networks (Sioshansi, 2016). Large-scale investment requirements can alter the cost structure and the use of inputs (operational and capital expenditures) by network companies. Network investments are also 'lumpy', implying increased uncertainty in benchmarking analysis. This is because investments are mostly irreversible and the future is uncertain (Dixit and Pindyck, 1994; Bruneekreft, 2013).

Addressing the concerns of inadequate supply security would also imply that incentive regulation is evolving from an *input-oriented* to an *output-oriented* approach. An *output-based* incentive regulation approach evaluates the monopoly’s performance in terms of the quantity and quality of delivered outputs, such as energy and connection services as well as service quality and provides incentives to improve quality (Vogelsang, 2006). However, the probable inclusion of additional output measures of performance such as network security is unexplored by regulators and scarcely discussed among academics and policymakers.

The aim of the paper is to illustrate how output measures of supply security performance such as ‘network security’ can be utilised using benchmarking analysis within an incentive regulation framework. We conceptualize ‘network security’ as encompassing the conventional elements of supply security, such as short-run operational reliability, commercial reliability, and long-run resource adequacy (see e.g. Joskow, 2007), along with security threats arising from natural, accidental and malicious (or exceptional) events facing the electricity network (see Nepal and Jamasb, 2013)[2]. The paper defines and designs a suitable output metrics of network security to be incorporated in an output-oriented incentive regulation framework. The paper also stimulates policy discussion on conceptual and technical aspects of incorporating network security in an incentive regulation framework using a benchmarking analysis.

The remainder of the paper is organised in four sections. Section 2 discusses the literature on the theoretical and empirical linkages between incentive regulation and network security by focussing on the regulation of quality of service in the European context. Quality of service is an integral but not the only component of network security (Nepal and Jamasb, 2013).

[2] According to CEER (2012), exceptional events include exceptional weather conditions and other exceptional circumstances that can significantly affect the continuity of supply. We share the same understanding of exceptional events in the remainder of the paper.

Section 3 focuses on general approaches to benchmarking analysis of network security with different benchmarking options, such as network security costs, network security cost drivers, data (or sample) size and quality, and the mathematical techniques. Section 4 proposes an output metrics for network security, critically reflects on the findings from the previous sections, and offers policy recommendations. Section 5 concludes the paper.

2. Relevant Literature Review

Electricity networks exhibit natural monopoly characteristics, such as economies of scale, scope and density due to high sunk costs and low marginal operating costs (Kahn, 1971). In the absence of regulatory interventions, network companies face low incentives for internal efficiency and greater incentives for rent-seeking, leading to distortions in allocative efficiency. Hence, incentive-based regulation (such as price cap or revenue cap regimes) of network entry, access and charges has been implemented in many European countries since the liberalisation of the electricity sector. Utility benchmarking under incentive regulation aims to promote economic efficiency (cost, allocative, and dynamic efficiencies) by reducing the regulated firm’s information advantage with its inputs and demand. It can thus be viewed as a second best solution to competitive markets (Newbery, 2002; Joskow, 2013).

Benchmarking can be a useful tool in assessing the efficiency and performance of the regulated company in meeting the productivity objectives defined by the regulator ex-ante (Ajodhia et al., 2004). The results from statistical benchmarking methods help to determine the relative efficiency of an individual company’s operating costs and service quality relative to their peers. This information can then be used as input for setting the initial price 'P_o' and the 'X' factors, reflecting the cost reduction path during a given regulatory period (Jamasb et al., 2004; Joskow, 2008). A robust benchmarking can aid the regulator in determining the relative efficiency of different network companies and in setting their reasonable targets in terms of cost efficiency (Coelli et al., 2008). Hence, benchmarking of network companies can play a key role in sharing the benefits of efficiency improvements with consumers and ensuring that regulated network companies earn a fair return on their investments (Haney and Pollitt, 2013).

From a theory point of view, the optimum level of network security (and service quality) is attained when a profit maximising regulated company increases network security to the point where the marginal benefit of additional network security equals the companies’ marginal cost of increasing security (see Sappington, 2005). Figure 1 presents a graphical representation of the optimum level of network security considering that the reliability level reflects the consumers' preferences. However, regulation of network security or other aspects of the security of electricity supply such as service quality suffers from three major problems (Spence, 1975; Fraser, 1994): a) the problem of measuring service quality; b) the lack of information on the actual consumer demand for service quality; and c) the lack of information on the efficient costs required to produce optimal service quality.

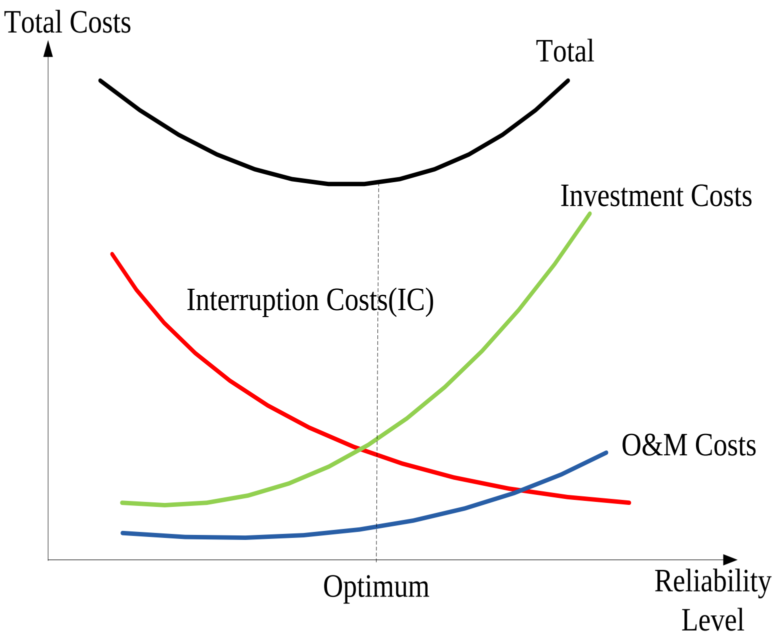

Figure 1: Socio-economic optimization of network security

In many European countries, service quality is treated under separate incentive schemes and rewards and penalty scheme (RPS) (CEER, 2012; Fumagalli, 2012). For example, in 2000, Italy introduced a RPS followed by Norway and Great Britain in 2001 and 2002 respectively, while France introduced an RPS in 2009. Under the RPS, the regulated tariff (or the allowed revenue) of the network company is increased (rewarded) or decreased (penalised) in proportion to the difference between the actual performance and target performance set by the regulator ex-ante and an incentive rate in the form of a monetary value per unit change in service quality. The RPS incentive structure is in line with the theory of optimal incentive scheme when quality is verifiable (Laffont and Tirole, 1989). The RPS scheme places importance on precisely identifying the underlying production technology of the network company to promote efficient delivery of service and quality (Coelli et al., 2013).

An alternative approach is to include network security aspects such as service quality into the efficiency benchmarking. This approach would imply that the efficiency requirement also includes incentives for service quality (and network security) improvements. Moreover, the cost efficiency or cost saving objectives of incentive regulation can adversely affect service quality (and network security) if the regulated prices are not allowed to increase, as the network company incurs greater costs to improve the service quality (Sappington, 2005). For example, empirical studies, such as Ter-Martirosyan (2003) and Ter-Martirosyan and Kwoka (2010) have shown that in the absence of appropriate quality controls, incentive regulation leads to deteriorating levels of service quality in the US electricity networks.

Only a few empirical studies based on panel and cross-sectional data have explicitly included service quality in benchmarking analysis in the European context while examining the effects of incentive regulation on service quality. Giannakis et al. (2005) used the data envelopment analysis (DEA) frontier method to measure technical efficiency (TE) based on non-parametric input distance functions and total factor productivity (TFP) growth among the UK's 14 distribution companies for the period 1991/92 to 1998/99. The results showed that cost-efficient firms did not necessarily exhibit high service quality, although it was desirable to integrate quality of service in benchmarking. Similarly, Yu et al. (2009) presented an empirical approach to measure and incorporate service quality into benchmarking analysis in the UK distribution networks from 1990/91 to 2003/04 using the DEA technique that extended the earlier research by Giannakis et al. (2005). The results showed that from a performance point of view, cost and quality were not separable and that there were potential trade-offs between costs and quality of service.

Coelli et al. (2008) estimated a benchmarking model incorporating a service quality parameter for the 92 French electricity distribution units of EDF for the period, 2003-2005. Using the SFA and DEA techniques with input distance functions, the results showed that inclusion of service quality had no significant effect on the mean TE scores, implying that including a quality indicator in efficiency benchmarking had no substantial effect. Growitsch et al. (2009) undertook an efficiency analysis of distribution networks from seven European countries applying the stochastic frontier analysis (SFA) method to multi-output translog input distance function models. The results showed significant potential trade-offs between quality and efficiency scores, especially for smaller network companies.

Some recent studies have examined the impact of quality of service regulation on the performance of network companies in terms of cost efficiency and quality provision using benchmarking analysis. Norway is a notable exception in integrating the cost of quality (in the form of the value of energy not delivered) in the efficiency benchmarking exercise. Growitsch et al. (2010) explored the impact of incorporating customers' willingness-to-pay for service quality in benchmarking models on cost efficiency of distribution networks in Norway using the DEA technique. The results showed that the introduction of service quality regulation had no conflict with and impact on the performance and cost efficiency of the network utilities.

In the UK electricity distribution, Jamasb et al. (2012), by specifying a new empirical model, showed that regulatory incentives to reduce service interruptions had not been sufficiently strong to achieve economically efficient levels of service quality. However, the economic incentives to encourage utilities to reduce network energy losses have led to performance improvements in this area.

Cambini et al. (2014) investigated the response of the largest Italian electricity distribution company to the input- and output-based incentives using a balanced panel for 115 companies spanning 2004 to 2009. A two-stage, semi-parametric DEA and bootstrapping techniques were applied. The main finding was that the presence of quality regulation did not significantly alter the behavior of the firms, implying that cost efficiency incentives did not conflict (or trade-off) with quality-related incentives.

The empirical evidence discussed so far suggests that the incorporation of network security in efficiency benchmarking is a relatively new concept and remains unexplored both in the academic literature and in regulatory practices. A first step towards including network security in benchmarking analysis would be to establish a conceptual benchmarking framework for network security. This presents a major knowledge gap which our study aims to bridge to some extent.

3. Benchmarking Frameworks

The incorporation of network security in benchmarking analysis typically involves identifying the network security-related 'inputs' (such as capital and operating expenditures of network security) and a range of network security-related 'outputs' (such as quality of service, e.g., duration and frequency of interruptions). A network company will then be regarded as being more efficient, in our case in delivering network security, if it is able to deliver more network security-related outputs while using less input factors.

Table 1 presents several considerations that arise in connection with integrating network security in a benchmarking framework. A benchmarking framework for network security has to consider four major dimensions: a) network security-related costs; b) network security-related cost drivers; c) the data sample; and d) the benchmarking technique. The benchmarking framework should identify and describe the conceptual aspects involved in benchmarking, along with the categorisation of different benchmarking techniques, as discussed below.

<table>
<tr><th>Network security-related costs</th><th>Network security-related costs drivers</th></tr>
<tr><td>• Top-down versus bottom-up approach
➢ If Top-down: Totex on network security versus (Opex + Return + Depreciation)
➢ Separate OPEX and CAPEX for network security
➢ By type of network security activities</td><td>• High level versus detailed
• Inclusion of metrics (or outputs)
• Exogenous variables</td></tr>
<tr><th>Data sample</th><th>Techniques</th></tr>
<tr><td>• Cross-section versus panel
• Historic data versus future plans
• International sample versus domestic sample</td><td>• Partial Performance Indicators (PPI)
• TFP and other index-based productivity approaches
• Norm and reference models
• Econometric methods (OLS /COLS/MOLS)
• Frontier methods
➢ DEA
➢ SFA</td></tr>
</table>

Table 1: Several considerations involved in benchmarking network security

3.1 Network security-related costs

Network utilities incur both operational expenditures (Opex) and capital expenditures (Capex) related to network security. Opex generally includes operating and maintenance costs (both variable and fixed) that the network company incurs during a fiscal year. Capex expenditures generate long-term future benefits and are incurred when a network company invests in new fixed assets to replace the existing old assets or to expand the network. There are several ways in which these costs can be structured, aggregated and treated in a benchmarking exercise under an input-based incentive regulation.

The *bottom-up* approach involves treating different types of costs (i.e. Opex and Capex) in different benchmarking analyses. The Opex can be an aggregate measure or split according to the type of network security-related activity (such as wages and salaries, repair costs etc.). Each type of cost enters a separate benchmarking model with different cost drivers. However, such activity-specific treatment of network security Opex in benchmarking gives rise to implementation issues, such as data-quality and data comparability. Effective Opex benchmarking requires harmonised rules for cost classifications and allocation that are consistently applied across the network companies. On the other hand, Capex benchmarking can pose difficulties due to significant heterogeneity between network companies in terms of the age of assets, geography, lumpiness of investments and other considerations (Joskow, 2008). The differences in the cost nature imply that a benchmarking approach to Opex may not be suitable for Capex.

The bottom-up approach to network security benchmarking may be suitable if the regulation framework is based on the 'building blocks' approach where the constituent components of total costs such as opex and capex are subject to scrutiny. However, the building blocks approach suffers from the 'double jeopardy' problem characterised by the allocative and accounting trade-offs between Capex and Opex (Ajodhia et al., 2006). A partial cost benchmarking under the bottom-up approach can lead to an overall estimate of costs, which can be unfeasible, and an unreasonable basis for setting targets, as the regulator combines the most efficient (or the lowest) costs for each subset from different network companies (Shuttleworth, 2005).

The *top-down* approach uses a comparison of total network security costs among network companies. The approach can involve controlling for the effects of contextual factors, such as economies of scale, scope and density and network topography. Benchmarking total expenditures (Totex) creates a more equal treatment of capital and operational expenditures in efficiency analysis, and is an alternative approach to overcoming the problems associated with the accounting treatment of capital expenditures. Moreover, an effective Totex benchmarking requires large datasets to minimise the aggregation problem as the transmission and distribution companies tend to invest in network security assets with a long service life. This is important, as network security Totex can constitute lumpy, indivisible, volatile and cyclical investments, which lead to wide short-term fluctuations in the annual value for Totex.

An alternative approach to Totex benchmarking is the total cost benchmarking. Total cost includes the sum of Opex plus the depreciation of capital and an allowed return on capital. Hence, total cost benchmarking, to some extent, addresses the challenges associated with capex benchmarking when investments are characterised by lumpiness and annual variability. For example, the total cost approach to benchmarking has been adopted by the Dutch and the Norwegian regulators in their regulation of transmission and distribution networks (Ajodhia et al., 2006). Total cost benchmarking creates incentives to improve security performance in both the short and long run. However, determining a suitable basis for depreciation of asset values (accounting, regulatory or economic) such as book values versus replacement costs, and calculating the return on capital can be problematic (Diewert, 2005). Overall, costs benchmarking requires standardised definitions and classifications of Opex and Capex, considering the differences in accounting classifications of costs across countries (Cohen, 2005).

From a social-welfare perspective, a regulator can also consider incorporating the costs of inadequate network security in the total cost estimates and undertake benchmarking analysis based on a measure of the social costs of network security. The Finish and Norwegian regulators have included the estimated socio-economic cost of outages (i.e., the value of energy not served due to outages) as part of the total cost for efficiency benchmarking (Kuosmanen, 2012). Outage costs are also used as an instrument to evaluate the social cost of service, including service quality. However, there is no consistency in estimating outage costs among the EU regulators. Assessing the costs of network security failure can be contentious and the information requirement is high considering the multi-faceted and infrequent nature of the problem as well as the limitations on data availability and quality.

3.2. Network security-related cost drivers

In economic and benchmarking modelling terms cost drivers are explanatory factors that drive the costs of network companies. Hence, it is desirable that the incentive regulation and benchmarking models can also reflect the network security. The incorporation of network security variables directly within a benchmarking model as 'outputs' can provide incentives to deliver these outputs at different cost levels. This is especially relevant given the European regulatory concerns with investment inadequacy, innovation and sustainability. Incentive regulation is also changing from an input-based to an output-based approach in countries such as the UK and Italy (Cambini et al., 2013). An output-oriented approach combines the efficiency mechanisms in a revenue cap framework with output-based incentives, including those concerning network security.

The primary cost drivers in network benchmarking can include demand and supply side variables, such as the number of connections (a proxy to reflect fixed costs), load served (a proxy for network capacity), volume of energy delivered (a proxy to reflect the cost of energy), network security variables, network energy losses and network length. The selection of cost drivers should ideally be independent of data availability considerations. For example, Turvey (2006) criticised the practice of choosing the number of cost drivers to suit the data. The use of available data on electricity distributed (MWh) as a proxy for maximum demand and on network length per customer as the customer density variable to explain maximum demand can be questioned since they are only useful at the sub-station level[3]. This is because the relevance of these measures depends on networks having similar customer and load factors. On the other hand, the inclusion of network length as an output variable can introduce perverse incentives by encouraging network expansion solely to improve relative performance (CEPA, 2003).

Coelli (2012) suggested that one possible approach to choosing the relevant cost drivers is to explore the implications of an engineering-based reference or norm model of network companies. For example, Burns et al. (2005) described a method previously used in Austria for selecting cost drivers based primarily on an engineering-based simulation model of a hypothetical distribution network. Jamasb and Soderberg (2009) highlighted the Network Performance Assessment Model (NPAM) previously used by energy regulators in Sweden, Spain, Peru and Chile. However, network security is generally unexplored in benchmarking

[3] If demand falls in one area, spare capacity can’t be ‘physically relocated’ to another area.

analysis, implying that the existence of a network security that defines the output indicator as a cost driver in benchmarking analysis is largely unknown.

The quality of service indicators that commonly enter the benchmarking models as explanatory variables are the continuity of supply indices, such as the System Average Interruption Duration Index (SAIDI) and the System Average Interruption Frequency Index (SAIFI). However, these indicators are generally inadequate for mimicking the impact of interruptions arising from exceptional events because exceptional events lead to long, unplanned interruptions (CEER, 2012). Hence, an alternative approach would be to construct a new SAIDI indicator that only accounts for unplanned interruptions of longer than 5 minutes (Jamasb and Nepal, 2015). Long, unplanned interruption of at least 5 minutes (which are relatively more frequent than major exceptional events) can mimic the impact of interruptions engendered by exceptional events. Also, while there is limited data on exceptional events, more data is available on long, unplanned interruptions. Furthermore, it is advisable to use an average measure over several years instead of annual values as exceptional events that are less frequent than short and planned interruptions. This would increase the stability of the network security indicator.

For the transmission system reliability, other output indicators such as 'unsupplied energy' or average interruption time (AIT) can be used. For example, Ofgem developed incentive mechanisms for different aspects of distribution network service quality in 2004. For example, a new incentive mechanism in the UK introduced in 2005 focused on transmission system reliability as measured by the value of energy not supplied (Ofgem, 2004). However, consistent cross-sectional and time-series data measuring different aspects of network security such as interruption statistics are generally not available, as network companies do not systematically report them. Improving data quality is possible when regulators are resourceful and invest the required time and effort.

3.3 Data samples

Data availability and quality are important for performing benchmarking analysis for the regulation of network security. Accessing larger datasets and improving data quality also increases the robustness of the benchmarking results (Lowry et al., 2005). Panel data is generally preferable than cross-sectional data in benchmarking analysis, as the results obtained from cross-sectional data do not reflect the longer-term security performance of the network. The benchmarking results from cross-sectional data may be influenced by exceptional, company-specific events such as one-off major security-related capital expenditure. Such results can be misleading in capturing the network security efficiency of the companies over time. Burns and Weyman-Jones (1996) found that panel data could address certain shortcomings of cross-sectional data, as some variables that are particularly important for cross-sectional comparison may not be required for a panel-data analysis.

However, the use of panel data in network security benchmarking poses certain problems. The availability of appropriate price deflators is a concern as the economic value for some security inputs needs to be deflated to derive the equivalent constant cost measures. Also, panel data may be inconsistent over time due to changes in definitions, accounting standards, or data providers. These can limit data comparability over time and across the network companies. Furthermore, using benchmarks based on historic costs to determine future revenue allowances can be less reliable than has been in the past, when the European electricity industry was in more of a steady state (Frontier Economics, 2010). This is especially relevant for network security, as the additional costs involved are uncertain in terms of magnitude and timing. For example, network companies can incur different costs at different times to achieve the security objectives. Hence, benchmarking historic security costs under increasing uncertainty are not likely to provide reliable and informative results.

An alternative to historic cost benchmarking is benchmarking based on future or forecasted network security costs. Assessment of planned total security costs against explanatory factors and future increases in the outputs of the networks make benchmarking more oriented towards improving consumer welfare (Frontier Economics, 2010). The threat of disallowance of security enhancing costs and regulatory risks of security assets stranding as a result of ex-post benchmarking is avoided under this approach. Instead, companies are required to meet set security targets at an efficient price. However, future cost benchmarking suffers from the risk of inflated costs by the companies (Jenkins, 2011). For example, the Information Quality Incentive (IQI) mechanism introduced by Ofgem addresses the incentive by the networks to inflate future costs even though it is unlikely to completely eliminate such incentives in practice among the companies. Hence, in the absence of long panel data on outputs, analysis of historic costs in benchmarking can provide an additional means of assessing future expenditure requirements.

International benchmarking offers another option to increase the sample size and dataset by including network companies that operate in other countries. This data enrichment can be especially useful in the benchmarking of transmission companies, given their limited number in a single country. This implies that the scope of benchmarking with the country-specific transmission companies is low, given their small numbers. For example, the UK has only three electricity transmission operators and one gas transmission operator. Studies by Agrell and Bogetoft (2009) and Jamasb and Pollitt (2003) on electricity and Jamasb et al. (2008) on gas transmission networks provide applications of international benchmarking on efficiency analysis and regulation of the transmission companies. However, international benchmarking involves issues, such as the availability and consistency of data, exchange rates and technical matters for addressing country differences in input price, such as labour, cost of capital, regulatory issues such as timing of rate reviews, and environmental factors (Jamasb and Pollitt, 2003; Haney and Pollitt, 2013). The trade-off between increasing the sample size and maintaining the homogeneity (or adjusting for heterogeneity) of the sample is another issue associated with international benchmarking.

3.4. Benchmarking techniques

There are different potential approaches to the benchmarking of network security. The choice of the method is crucial as it can influence the results significantly. Coelli (2012) describes five common benchmarking methods in detail after reviewing the energy regulatory practices in 15 OECD countries. The benchmarking methods comprise the Partial Performance Indicator (PPI) method, Index-number-based Total Factor Productivity (TFP) analysis, the Econometric method (EM), Stochastic Frontier Analysis (SFA), and Data Envelopment Analysis (DEA).

The PPI method involves the use of trend or ratio analysis of the network companies' inputs or outputs, and makes comparisons on the efficiency performance with other networks or an industry average (Stone, 2002). This method calculates a single explanatory variable, and the indicators produced are generally easy to compute. The data requirements are not high and the results are simple to interpret and, therefore, require less data, while the results obtained only suggest significant cost differences that exist between network companies. However, as a partial indicator it is not able to simultaneously account for multiple inputs.

The TFP is a ratio of a measure of total output to a measure of total input use that reflects the overall productivity change (Turvey, 2006). The TFP method is best used to measure the productivity performance of a single or a group of network companies over time. There are alternative methods for measuring TFP growth, including non-parametric approaches, such as index numbers and DEA, and parametric approaches, such as Stochastic Frontier Analysis (SFA) and econometric cost-function models. The Index-number-based TFP is commonly used for measuring productivity growth when there are a limited number of observations available (Fisher, 1922; Diewert, 1992). However, the index-number-based TFP method is demanding in terms of information requirement as it requires price and quantity information on the inputs and outputs for two or more network companies over long time periods. Austria and Germany have used the TFP method to assess the performance of the electricity distribution companies in measuring the general productivity trend.

The econometric methods (EMs) involve the use of a cost function, which shows the output-cost relationship for cost minimising, or profit maximising network companies. A minimum-cost function provides the periodic costs incurred by an efficient network company to deliver the network services by modelling the technology in place, the output quantities, the input prices, and the operating conditions of the company (Coelli et al., 2005). Least-squares-type estimations such as ordinary least squares (OLS), corrected ordinary least squares (COLS) or modified ordinary least squares (MOLS) are used to estimate the parameters of the cost function for comparable companies under this approach (Richmond, 1974). The results are then used to derive the expenditures required by individual companies if they are minimising costs (i.e. the 'benchmark cost') and need to be compared with their observed costs for benchmarking purposes. The difference in the observed cost from the benchmark cost is largely attributable to management or controllable inefficiency. Hence, the EMs do not allow for a separate random error term from the inefficiency terms in the modelling while they also require specification of a correct functional form. UK and Ireland have used the EMs in electricity distribution in additional and supporting analyses.

SFA is an extended parametric econometric method that is used in cost benchmarking. The technique enables the estimation of a cost frontier from which actual costs incurred by the network can be compared. However, it differs from traditional econometric approaches in two important ways (Schmidt, 1976). SFA focuses on estimating the cost frontier representing the minimum costs rather than estimating the cost function representing the 'average' network company. SFA also separates the random statistical noise from the estimation of inefficiency by separating the composite residuals into two components consisting of a random error term and a term capturing 'other departures from the frontier'. The terms capturing 'other departures from the frontier' are assumed to be management-controllable inefficiencies. SFA has been used in Germany, Finland and Sweden.

On the other hand, DEA is a non-parametric technique that can compare the efficiency and productivity of companies that produce similar outputs using similar inputs. Unlike parametric techniques, DEA does not require ex-ante assumptions about the shape of the underlying production function or cost function (Coelli et al., 2005). Information about the shape of the real-world production technology is inferred from observations of the input-output combinations used by the businesses. However, as a deterministic method, DEA results are sensitive to outlying observations. DEA has been applied by energy regulators in Finland, Norway, the Netherlands, Germany and Austria.

Figure 2 shows the data and information requirements for different benchmarking techniques reflecting differences in the comprehensiveness and accuracy of methods along the spectrum of simplicity to complexity. PPI has limited data requirements and is less complicated while TFP is information-intensive, as it requires both price and quantity information on inputs and outputs, which makes the technique more complicated. The other three methods (EMs, SFA and DEA) are more effective with larger samples and lie between the two extremes of the spectrum.

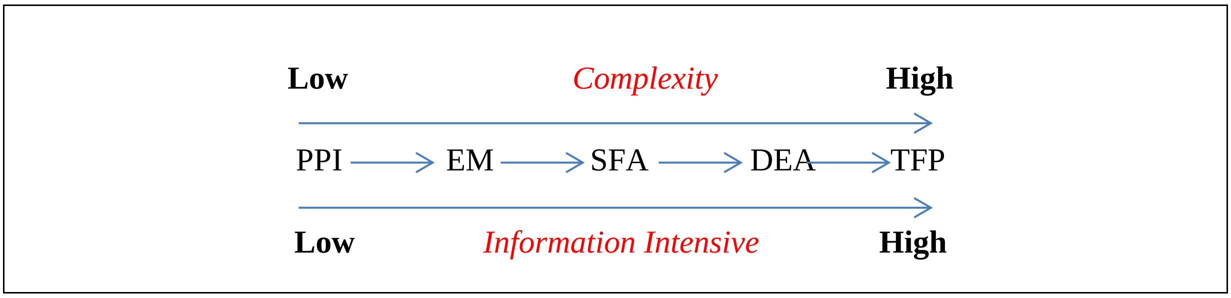

Fig 2: Data requirements and complexity of different benchmarking techniques

Table 2 shows the general properties of the different benchmarking techniques. SFA seems to be the most complete approach, being relatively strong on both theoretical and statistical grounds and, hence, the most suitable candidate technique for benchmarking of network security costs.

Properties \ Techniques	PPI	TFP	EM	SFA	DEA
Type	Non-parametric	Non-parametric	Parametric	Parametric	Non-parametric
Presence of random error	No	No	Yes (one composite error term)	Yes	No
Presence of inefficiency	No	No	Yes (one composite error term)	Yes	Yes
Presence of optimal behaviour	No	Yes	Yes (cost function)	Yes (cost frontier)	Yes (frontier firms)
Number of inputs	Single	Multiple	Multiple	Multiple	Multiple
Number of outputs	Single	Multiple	Multiple	Multiple	Multiple
Data requirements	Cross sectional or time series	Cross sectional or time series or panel	Cross sectional or time series or panel	Cross sectional or panel	Cross sectional or panel

Table 2: General properties of benchmarking techniques
Source: Adapted from Coelli (2012)

4. Alternative Approach and Discussion

The review of the benchmarking methods suggests that undertaking robust benchmarking of network security can pose challenges to energy regulators. The main challenge stems from the confusion surrounding the treatment, accounting and classification of different types of security costs, the choice of appropriate variables to include as cost drivers and, most importantly, the lack of comprehensive and quality data related to network security. Nonetheless, network security output indicators can be defined and designed while considering the existing data limitations, and incorporated in an incentive regulation framework. Our proposal to incorporate network security in incentive regulation framework by designing a network security output indicator is explained next.

A network security metrics can be designed by including long, unplanned interruptions of at least 5 minutes (which are more frequent than exceptional events). Long, unplanned interruptions can mimic the impact of interruptions engendered by exceptional events since interruptions from such events are often long and affect many customers. Using the long, unplanned interruptions also increases data availability for benchmarking analysis to derive the metrics. Hence, the allowed revenue or price path (P_t) of the regulated network company can be directly linked to the network security indicator in an incentive regulation framework where RPI is the retail price index, and X is the efficiency gain (or the efficiency factor). Q* is the network security adjustment parameter (or the network security output indicator) and is defined as an output measure of the continuity of supply (or service quality) for long, unplanned interruptions of at least 5 minutes. The annual values of Q* are calculated from benchmarking, ex-post on the basis of the companies' performances, and can take a negative or a positive sign. A positive value of Q* implies that network security has improved more than required at the national level.

$$P_t = P_{t-1} (1 + RPI - X + Q^*)$$

However, the adoption of statistical methods to account for exceptional events requires harmonisation of network security indicators and data collection procedures. This can be problematic in Europe because the understanding and definition of exceptional events varies between the EU member countries, where some countries adopt a more statistical approach while others qualitatively define exceptional events in terms of their causes (CEER, 2012). Not all EU countries share interruption statistics arising from exceptional events in their interruption database, such as Germany, Denmark and the UK. From a benchmarking perspective, it is desirable that interruption statistics from exceptional events are recorded and shared among the members. These factors also complicate the international benchmarking of network security in Europe.

The results from benchmarking, if undertaken, may be inaccurate in the absence of adequate, good quality data pertaining to network security. The results may be informative and not deterministic from a regulatory perspective. Most importantly, undertaking network security benchmarking with limited data leads to inaccurate results while the costs of implementing it incorrectly are high, considering the distortions in large-scale future investments pertaining to network security. Hence, the need to design alternative approaches to treat large-scale security costs arises within incentive regulation. This is because incentive regulation is a paradigm while benchmarking is a tool which incentive regulation may embrace.

Network security costs capitalisation and *network security cost pass-through* are two input-based approaches to treat network security costs within incentive regulation but are not subject to benchmarking. Capitalisation implies that security costs are treated as capital expenditures (i.e. cost capitalisation) and are included in the regulatory asset base (RAB) and depreciated in line with other assets. Network companies can earn a rate-of-return (or possibly extra rate-of-return) on network security-related capital expenditures, irrespective of security and efficiency improvements achieved.

Cost pass-through involves treating the costs related to network security by passing them on to final consumers, assuming that the regulator accepts network security costs in the regulatory asset base (RAB). Hence, network security costs are treated as operational expenditures (Opex) of the network companies and are subject to direct pass-through under this approach. However, the regulator should cap or ex-ante approve the security costs to be capitalised or passed-through to mitigate the gold-plating of network security costs.

The risks associated with large-scale and irreversible network security investments suggest that these investments can undergo the initial regulatory scrutiny and receive ex-ante approval or refusal For example; the RIIO (Revenue=Incentives+ Innovation + Outputs) model to be adopted in the UK requires that budget allowances undergo ex-ante regulatory approval. There are two regulatory tests determining the 'usefulness' and 'efficiency' of investments (Joskow, 2008; Brunekreeft, 2013). These ex-ante tests allow the regulator to detect whether a particular security investment is useful and whether investment is realised at an efficient cost.

From a welfare economic perspective, the 'usefulness' test can be conducted by using a cost-benefit analysis (CBA) as a systematic approach for calculating and comparing the benefits and costs of security investments in determining whether investments are justified and feasible. It involves comparing the total expected cost of each investment option to network security against the total benefits. Hence, an investment is useful if the benefits outweigh the costs (i.e. net benefit is positive). A social cost benefit analysis (SCBA) can also be carried out, although pricing the externalities arising from network security investments becomes a critical issue.

The CBA framework on network security should account for the high-impact, low frequency nature of exceptional events. By definition, exceptional events are central to the concept of network security. Policy conclusions that do not comprehensively account for exceptional events in a CBA of network security are incomplete. One possible approach to consider exceptional events such as the network security of CBA is by conducting a probabilistic or stochastic CBA (Azar and Lindgren, 2003). This approach assigns probabilities for the occurrence of exceptional events to estimate the expected benefits and costs. However, estimating realistic probabilities for exceptional security events and estimating the benefits of the correct or required level of investments is a major challenge and can test the suitability of SCBA to its limit.

An alternative approach to assessing the usefulness and efficiency of network security investments is to undertake a cost-effectiveness analysis (CEA) of the required investments. A CEA analysis of security investments identifies the most economic or efficient way to undertake a given network security investment. CEA can provide an ex-ante evaluation to support decision-making that relates to network security and guides the choices to be made by decision makers. However, both CBA and CEA analyses of network security investments need to be accompanied with a sensitivity analysis in order to validate and increase the robustness of the results.

5. Conclusions

The novelty of the present paper is that it discussed and proposed the possible incorporation of network security in a benchmarking analysis within an incentive regulation framework. The need for large investments in achieving the European energy policy goals of sustainability, economic efficiency and security of supply places emphasis on the adaption and development of benchmarking as a useful tool for incentive regulation. This paper discussed the different considerations when benchmarking network security costs. We underscored the issues and options associated with different benchmarking approaches in terms of costs, cost drivers, data and techniques pertaining to network security.

We discussed that network security cost benchmarking requires a clear understanding of the cost structure of networks. The need to understand the key security outputs provided by benchmarked companies along the network inputs used (and their price) and other associated exogenous variables such as key environmental factors remains crucial. The effectiveness of the use of more sophisticated techniques for network security costs benchmarking tends to be greater with the availability of relevant data. The use of panel data techniques to deal with unobserved heterogeneity among the networks and the validity of the relevant comparator group in security benchmarking is also likely to depend on data availability.

We also highlighted the accounting and classification issues of security costs, choice of cost drivers, data adequacy and quality and the choice of benchmarking techniques. Assembling and sharing of international datasets can mitigate data availability if compatible international data are available together with a proper understanding of the practical issues involved when using international data to benchmark domestic network companies.

The use of network security costs benchmarking can be initially helpful as an informative rather than a deterministic tool in the incentive regulation of network security. However, network security costs can also be dealt with outside benchmarking but within an incentive regulation framework through cost capitalisation and costs pass-through. Stochastic CBA and CEA can be helpful to the regulator in assessing the usefulness and efficiency of network security investments. These approaches can complement each other and provide valuable information to the regulator with regards to the treatment of network security costs in an incentive-based regulatory framework.

References

Agrell, P. and Bogetoft, P. (2009). International Benchmarking of Electricity Transmission System Operators, e3grid project, Final Report, September.

Ajodhia, V., Petrov, K. and Scarsi, G.C. (2004). Quality, Regulation and Benchmarking – An Application to Electricity Distribution Networks, *Zeitschrift for Energiewirtschaft*, 29(2), pp. 107-120.

Ajodhia, V., Kristiansen, T., Petrov, K. and Scarsi, G.C. (2006). Total Cost Efficiency Analysis for Regulatory Purposes: Statement of the Problem and Two European Case Studies, *Competition and Regulation in Network Industries*, 1(2), pp. 263-286.

Armstrong, C.M., Cowan, S., and Vickers, J. (1994). Regulatory Reform, Economic Analysis and British Experience, Cambridge, MA: MIT Press.

Azar, C. and Lindgren, K. (2003). Catastrophic Events and Stochastic Cost-Benefit Analysis of Climate Change, *Climatic Change*, 56(3), pp. 245-255.

Brunekreeft, G. (2013). On the Role of International Benchmarking of Electricity Transmission System Operators Facing Significant Investment Requirements, *Competition and Regulation in Network Industries*, 30(1), pp. 1-22.

Burns, P., Jenkins, C. and Reichmann, C. (2005). The Role of Benchmarking for Yardstick Competition, *Utilities Policy*, 13, pp. 302-309.

Burns, P. and Weyman-Jones, T. (1996). Cost Functions and Cost Efficiency in Electricity Distribution: A Stochastic Frontier Approach, *Bulletin of Economic Research*, 48(1), pp. 41-64.

Cambini, C., Croce, A. and Fumagalli, E. (2013). Incentives in Vain? Output-based Incentive Regulation and Quality in Electricity Distribution, 2nd. Conference on the Regulation of Infrastructure Industries, Florence, 07 June.

Cambini, C., Croce, A. and Fumagalli, E. (2014). Output-Based Incentive Regulation in Electricity Distribution: Evidence From Italy, *Energy Economics*, Vol. 45, September, pp. 205-216.

CEER (2012). Fifth CEER Benchmarking Report on the Quality of Electricity Supply, Council of European Energy Regulators, April, Brussels.

Celin, A. and Yalcin, N. (2012). Performance Assessment of Turkish Electricity Distribution Utilities: An Application of Combined FAHP/TOPSIS/DEA Methodology to Incorporate Quality of Service, *Utilities Policy*, 23, pp. 59-71.

CEPA (2003). Background to Work on Assessing Efficiency for the 2005 Distribution Price Control Review – Scoping Study: Final Report, Cambridge Energy Policy Associates, September.

Coelli, T.J., Rao, D.S.P., O'Donnell, C.J. and Battese, G.E. (2005). An Introduction to Efficiency and Productivity Analysis, 2nd Edition, Springer: New York.

Coelli, T., Crespo, H., Paszukiewicz, A., Perelman, S., Plagnet, M.A and Romano, E. (2008). Incorporating Quality of Service in Benchmarking Model: An Application to French Electricity Distribution Generators, Draft, June.

Coelli, T. (2012). Benchmarking Capex and Opex in Energy Networks, Working Paper No. 6, Australian Competition and Consumer Commission, May.

Coelli, T., Gautier, A., Perelman, S. and Saplacan, R. (2013). Estimating the Cost of Improving Quality in Electricity Distribution: A Parametric Distance Function Approach, *Energy Policy*, 62, February, pp. 287-297.

Cohen, J (2005). *Intangible Assets: Valuation and Economic Benefit*, John Wiley and Sons.

Diewert, W. (1992). Fisher Ideal Output, Input and Productivity Indexes Revisited, *Journal of Productivity Analysis*, Vol. 3, pp. 221-248.

Diewert, W. (2005). Issues in the Measurement of Capital Services, Depreciation, Asset Price Changes, and Interest rates, in Corrado, C., Haltiwanger, J. and Sichel, D. (eds), Measuring Capital in the New Economy, NBER Books, National bureau of Economic Research.

Dixit, A.K. and Pindyck, R.S. (1994). Investment under Uncertainty, Princeton University Press, Princeton, New Jersey.

ENTSOE (2012). Ten Year Network Development Plan 2011-2020, European Network of Transmission System Operators, Brussels, Belgium.

EURELECTRIC (2012). European Commission "Proposal for a Regulation on guidelines for trans- European energy infrastructure and repealing Decision no. 1364/2006/EC" (2011/0300 (COD)) of 19 October 2011, A EURELECTRIC Response Paper, January.

Fisher, I. (1922). *The Making of Index Numbers: A Study of Their Varieties, Tests and Reliability*, Houghton-Mifflin, Boston.

Fraser, R. (1994). Price, Quality and Regulation: An Analysis of Price Capping and the Reliability of Electricity Supply, *Energy Economics*, 16(3), pp. 175-183.

Frontier Economics (2010). RPI-X@20: The Future Role of Benchmarking in Regulatory Reviews, A Final Report Prepared for Ofgem, May.

Fumagalli, E. (2012). Service Quality Regulation: Framework and Experience, Florence School of Regulation, Residential and E-learning Course on Regulation of Energy Utilities, Florence, October.

Giannakis D., Jamasb, T and Pollitt, M. (2005). Benchmarking and Incentive Regulation of Quality of Service: An application to the UK electricity Distribution Networks, *Energy Policy*, 33, pp. 2256–2271.

Growitsch, C., Jamasb, T. and Pollitt, M. (2009). Quality of Service, Efficiency and Scale in Network Industries: An Analysis of European Electricity Distribution, *Applied Economics*, Vol. 41(20), pp. 2555-2570.

Growitsch, C., Jamasb, T., Muller, C. and Wissner, M. (2010). Social Cost Efficient Service Quality- Integrating Customer Valuation in Incentive Regulation: Evidence from the Case of Norway, *Energy Policy*, 38(5), pp. 2536-2554.

Haney, A.B. and Pollitt, M. (2013). International Benchmarking of Electricity Transmission by Regulators: A Contrast between Theory and Practice? *Energy Policy*, 62, November, pp. 267-281.

Jamasb, T. and Pollitt, M. (2000). Benchmarking and Regulation: International Electricity Experience, 9(3), pp. 107-130.

Jamasb, T. and Pollitt, M. (2003). International Benchmarking and Regulation: An Application to European Electricity Distribution Utilities, *Energy Policy*, 31(15), pp.1609-1622.

Jamasb, T., Nillesen, P. and Pollitt, M. (2004). Strategic Behaviour under Regulatory Benchmarking, *Energy Economics*, Vol. 26(5), pp. 825-843.

Jamasb, T., Pollitt, M. and Triebs, T. (2008). Productivity and Efficiency of US Gas Transmission Companies: A European Regulatory Perspective, *Energy Policy*, Vol. 36(9), pp. 3398-3412.

Jamasb, T. and Soderberg, M. (2010). The Effects of Average Norm Model Regulation: The Case of Electricity Distribution in Sweden, *Review of Industrial Organization*, Vol. 36(3), pp. 249-269.

Jamasb, T., Orea, L. and Pollitt, M. (2012). Estimating the Marginal Cost of Quality Improvements: The Case of the UK Electricity Distribution Companies, *Energy Economics*, Vol. 34(5), pp. 1498-1506.

Jamasb, T. and Nepal, R. (2015). Issues and Options in the Economic Regulation of European Network Security, *Competition and Regulation in Network Industries*, Vol. 16(1), pp. 2-22.

Jenkins, C. (2011). RIIO Economics: examining the economics underlying Ofgem's new regulatory framework, Presented to CCRP Winter Workshop, February.

Joskow, P.L. (2007). Supply Security in Competitive Electricity and Gas Markets, In C. Robinson (Ed.), *Utility Regulation in Competitive Markets*, Edward Elgar.

Joskow, P.L. (2008). Incentive Regulation and its Application to Electricity Networks, *Review of Network Economics*, Vol. 7(4), pp. 547-560.

Joskow, P.L. (2013). Incentive Regulation in Theory and Practice: Electricity distribution and Transmission Networks, NBER Chapters, in Economic Regulation and Its Reform: What Have We Learned? National Bureau of Economic Research, Inc.

Kahn, A.E. (1971). The Economics of Regulation: Institutional Issues, Vol. 2, Wiley: New York.

Kuosmanen, T. (2012). Stochastic Semi-Nonparametric Frontier Estimation of Electricity Distribution Networks: Application of the StoNED Method in the Finnish Regulatory Model, *Energy Economics*, Vol. 34(6), pp. 2189-2199.

Laffont, J.-J. and Tirole, J. (1993). A Theory of Incentives in Regulation and Procurement, MIT Press: Cambridge, MA.

Lowry, M., Getachew, L. and Hovde, D. (2005). Econometric Benchmarking of Cost Performance: The Case of US Power Distributors, *The Energy Journal*, Vol. 26(3), pp. 75-92.

Nepal, R. and Jamasb, T. (2013). Security of the European Electricity Systems: Conceptualizing the Assessment Criteria and Core Indicators, *International Journal of Critical Infrastructure Protection*, Vol. 6(3-4), pp. 182-196.

Newbery, D. (2002). Privatisation, Restructuring and Regulation of Network Utilities, MIT Press, Cambridge, Massachusetts.

Ofgem (2004). Electricity Distribution Price Control Review: Initial Proposals, Office of Gas and Electricity Markets, 145/04, June, London.

Pollit, M. and Haney, A. B. (2013). Dismantling a Competitive Electricity Sector: The U.K.'s Electricity Market Reform, *The Electricity Journal*, Vol. 26 (10), pp. 8-15.

Sappington, D. (2005). Regulating Service Quality: A Survey, *Journal of Regulatory Economics*, Vol. 27(2), pp. 123-154.

Schmidt, P. (1976). On the Statistical Estimation of Parametric frontier Production Functions, *The Review of Economics and Statistics*, Vol. 58, No. 2, pp. 238-239.

Shleifer, A. (1985). A Theory of Yardstick Competition, *RAND Journal of Economics*, Vol. 16, pp. 319-327.

Shuttleworth, G. (2005). Benchmarking of Electricity Networks: Practical Problems with its Use for Regulation, *Utilities Policy*, Vol. 13, pp. 310-317.

Sioshansi, F.P. ed. (2016). *Future of Utilities – Utilities of the Future: How Technological Innovations in Distributed Generation Will Reshape the Electric Power Sector*, Elsevier.

Spence, A.M. (1975). Monopoly, Quality and Regulation, *Bell Journal of Economics*, Vol. 6, pp. 417-429.

Stone, M. (2002). How Not to Measure the Efficiency of Public Services (and how one might), *Journal of the Royal Statistical Society: Series A*, Vol. 165(3), pp. 405-434.

Ter-Martirosyan, A. (2003). The Effects of Incentive Regulation on Quality of Service in Electricity Markets. Working Paper, Department of Economics, George Washington University.

Ter-Martirosyan, A. and Kwoka, J. (2010). Incentive Regulation, Service Quality, and tandards in U.S. Electricity Distribution. *Journal of Regulatory Economics*, Vol. 38, pp. 258–273.

Turvey, R. (2006). On Network Efficiency Comparisons: Electricity Distribution, *Utilities Policy*, Vol. 14, pp. 103-113.

Vogelsang, I. (2006). Electricity Transmission Pricing and Performance-Based Regulation, *The Energy Journal*, Vol. 27(4), pp. 97-126.

WIK-Consult (2011). *Cost Benchmarking in Energy Regulation in European Countries – Final Report*, Study for the Australian Energy Regulator, 14 December.

Yu, W., Jamasb, T. and Pollitt, M. (2009). Willingness-to-Pay for Quality of Service: An Application to Efficiency Analysis of the UK Electricity Distribution Utilities, *The Energy Journal*, Vol. 30(4), pp. 1-48.